STROOCK
SPECIAL BULLETIN

California Enacts Broad-Reaching Consumer Privacy Legislation

June 28, 2018

With Governor Jerry Brown's signature this afternoon, the California legislature passed the most sweeping privacy legislation in the Nation, to avert what promised to be a wildly expensive and contentious showdown over a competing – and more controversial – initiative slated for the November ballot (the "Privacy Initiative"). The California Consumer Privacy Act of 2018 (the "Act") imposes upon businesses within its coverage major new compliance requirements and liability exposure. The Act's provisions go into effect on January 1, 2020. The Act requires businesses to implement a new infrastructure to provide California residents with extensive controls over virtually every conceivable form of personal information, including the rights to prevent the sale and to require deletion of their information. It also increases the exposure for any data breach. This Bulletin summarizes key aspects of the Act and highlights key differences between the Act and the Privacy Initiative and the European General Data Protection Regulation ("GDPR") that went into effect on May 25, 2018.

The Act's Requirements

The Act applies to personal information concerning natural persons who are California residents. It defines personal information expansively to include not only traditional personally identifiable information, but also such far ranging categories as purchasing history or tendencies, records of products or services provided, biometric data, geolocation data, and "audio, electronic, visual, thermal, olfactory, or similar information," "psychometric information" and any inferences drawn from any such information. The inclusion of "inferences" drawn from the enumerated categories of personal information casts a virtually uncircumscribed net and could broadly affect the data analytics operations (e.g., customer profiling) that pervade today's businesses. Personal information does not include information that is "de-identified," a term that the state Attorney General is authorized to redefine as technology evolves.

The Act grants California consumers: (1) the right to know what personal information is being collected, whether it is sold or disclosed, and to whom; (2) the right to access and seek disclosure of personal information a business has collected; (3) the right to opt out of the sale of personal information; and (4) the right to require deletion of personal information a business has collected. Further, the Act prohibits businesses from discriminating between consumers based on their exercise of any of these rights, which means that businesses also cannot offer premium, free or

discounted products and services in exchange for the right to retain or sell consumers' personal information. In furtherance of these new rights, the Act requires that businesses provide two or more designated methods for submitting disclosure, deletion, and opt-out requests, including, at a minimum, a toll-free telephone number, and if the business maintains a website, a website address. With respect to opt-out requests, a business must provide a clear and conspicuous hyperlink on its Internet homepage titled "Do Not Sell My Personal Information" that enables the consumer to opt out of such sale.

The Act also imposes certain affirmative obligations on businesses within its coverage in relation to these new rights. First, at or before collection of personal information, businesses must inform consumers as to the categories of information collected and the purposes for which it will be used. Second, businesses must disclose to consumers that consumers have the right to request deletion of their personal information. Third, a business must, at least annually, update its online privacy policy (if it has one), as well as include the following in any California-specific description of consumer privacy rights: (a) a description of the consumer's rights under the Act; (b) categories of personal information it has collected in the preceding 12 months; (c) categories of personal information it has sold within the preceding 12 months, or that it has not sold such information; and (d) categories of personal information it has disclosed within the preceding 12 months, or that it has not disclosed such information.

In addition, the Act imposes numerous other compliance obligations on businesses, affecting everything from employee training to the provisions of contracts with entities with which they share consumer information. In a provision highly critical to businesses' risk exposure, the Act imposes liability for the unauthorized access and exfiltration, theft or disclosure of personal information as a result of a business' failure to implement "reasonable security procedures." The liability risk is high given the lack of definition around what constitutes "reasonable security procedures" and the negative inferences often drawn following a significant breach.

Businesses Covered Under the Act

The Act's provisions sweep a much broader base of businesses under its requirements than the Privacy Initiative would have. It applies to entities that do business in California and collect consumers' personal information, or on behalf of whom consumer personal information is collected (i.e., entities that employ a third party to collect consumer personal information), and satisfies one or more of the following thresholds: (a) annual gross revenues in excess of $25M (as opposed to the Privacy Initiative's $50M threshold); (b) alone or in combination annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices, (as opposed to the Privacy Initiative's 100,000 threshold); or (c) derives 50% or more of its annual revenues from selling consumers' personal information. The Act also applies to any entity that controls or is controlled by a business that otherwise satisfies these criteria, and that shares common branding with such a business. With Californians comprising roughly 12% of the U.S. population, covered businesses will have to decide whether to implement separate processes for handling the personal information of California residents, or apply these new standards nationwide.

Exemptions under the Act are few. The Act's provisions cannot restrict a business' ability to comply with federal, state, or local laws. It expressly excludes personal information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act to the extent the Act conflicts with that law. The Act also would not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report, and use of that

information is limited by the Fair Credit Reporting Act. Other exceptions include compliance with federal, state, or local law enforcement investigations or cooperation with law enforcement.

Another very narrow exception applies if every aspect of a business's collection or selling of California residents' personal information takes place wholly outside of California. This narrow exception only applies where no personal information is collected while the consumer is in California and no part of the sale of the consumer's personal information occurs in California.

With respect to California consumers' right to request deletion of personal information, a business shall not be required to delete personal information that is necessary for the business to: (1) complete the transaction for which it is collected, or provide the good or service requested by the consumer, or reasonably anticipate within the context of the business' ongoing relationship with the consumer; (2) detect security incidents and prosecute those responsible for such activity; (3) enable solely internal uses that are reasonably aligned with the consumer's expectations based on the consumer's relationship with the business; or (4) to otherwise use such information internally, in a lawful manner that is compatible with the context in which the consumer provided that information.

Enforcement of the Act

According to Senator Hertzberg, whose office led compromise efforts with backers of the Privacy Initiative, the most significant issue with the Privacy Initiative was the broad potential for liability in the form of consumer suits. A chief difference between the Privacy Initiative and the Act is that the Act eliminates the private right of action provided by the Initiative, vesting enforcement authority exclusively in the Attorney General, except in the case of data breaches.

Specifically, the Act provides for a private right of action for statutory damages (capped at $750 per consumer per violation – compared to the Privacy Initiative's provision for $1,000 per violation, and $3,000 per willful violation) only in the case of a consumer whose nonencrypted or nonredacted personal information is the subject of a data breach as a result of a business' failure to implement reasonable security procedures. Moreover, prior to bringing such an action, a consumer must provide 30 days' notice to the business of the alleged violation, with the business having an opportunity within that 30 days to cure. This provision is similar to the notice and cure provision in California's Consumers Legal Remedies Act. (While it is difficult to imagine how a business would cure a data breach in response to a notice and cure notification from a consumer, the notice may provide an alert that would facilitate mitigation efforts.) After complying with the notice and cure provision, the consumer also must notify the Attorney General within 30 days of filing suit. The consumer may only proceed with the action if the Attorney General takes no action in response to the notice within 30 days, or if the Attorney General advises within 30 days that he or she will prosecute an action but takes no steps to prosecute within six months. The Act also does away with the Privacy Initiative's provision that a mere violation of its provisions shall be deemed to constitute an injury in fact, regardless of pecuniary loss.

All other authority for enforcement of alleged violations is vested exclusively in the Attorney General in the form of a civil action for civil penalties. Civil penalties are to be assessed in accordance with Section 17206 of the California Business and Professions Code, and shall not exceed $2,500 for each violation, or, in the case of a willful violation, $7,500 for each violation. Twenty percent (20%) of any civil penalties awarded, or the proceeds of any settlement of such an action, shall be allocated to the Consumer Privacy Fund, to be created by the Act, with the remaining eighty percent (80%) allocated to the jurisdiction on whose behalf the action was brought.

Relation to the GDPR

While the Act moves California closer to the stringent data protection requirements of the GDPR, there are several key differences.

The GDPR focuses on regulating businesses' collection of personal data to ensure consumer privacy. Data may only be collected for legitimate purposes, and businesses are prohibited from processing personal data outside of the legitimate purpose for which it was collected. Moreover, businesses may not request personal data beyond that which is necessary to effect the purposes for which it is collected, and are required to delete such data once the purpose for which it was collected is fulfilled. Further, the GDPR requires that data subjects provide affirmative consent for any use of collected data beyond that for which it was collected. The GDPR also requires businesses to design systems that collect and store personal data with technological mechanisms in place so as to ensure the protection of such data. In addition, the GDPR requires that businesses subject to its jurisdiction provide a privacy notice to data subjects.

The Act shares some similarities with the GDPR's rights and requirements. Namely, both provide a right to obtain from businesses the categories of data collected and the purpose for the collection. And both the GDPR and the Act provide a right to receive not only the categories of personal information collected, but also the specific personal information collected and stored. Further, both the GDPR and the Act establish a right to request deletion of personal information collected (referred to in the GDPR as the "Right To Be Forgotten"). However, apart from the affirmative consent requirement, the GDPR contains no separate provision establishing a right to request that personal information not be sold, found in Act. Moreover, while the GDPR requires that businesses subject to its jurisdiction proactively send privacy notices to data subjects, the Act does not impose privacy notice requirements beyond those under existing law, other than requiring that businesses notify consumers of certain rights under the Act and periodically update their existing policies and notices. Rather, the Act places the onus on consumers to exercise the rights created thereunder and affirmatively request disclosure. Nor does the Act require, as the GDPR does, that businesses which collect large scale personal information of California residents employ a Data Protection Officer to ensure internal compliance with regulations.

Some provisions of the Act go beyond those of the GDPR. The Act's definition of personal information is far more sweeping than that of the GDPR in its inclusion of such categories as "audio, electronic, visual, thermal, olfactory, or similar information," geolocation data, "psychometric information" and any inferences drawn from any such information. Further, the Act precludes businesses from offering free or discounted versions of their services (e.g., a free or discounted app) in exchange for granting the business the right to market personal information collected, or a paid version that brings with it no right to market such information. The GDPR contains no such prohibition.

In short, despite being a slight improvement over the withdrawn Privacy Initiative (especially in providing additional time for implementation and scaling back the threat of private litigation), the Act imposes major new data protection burdens and risks on businesses that collect any form of personal information concerning California consumers. The Initiative, if adopted, would have required a 70% supermajority in each house of the California legislature, as well as the governor's signature, to change – a possibly insurmountable obstacle. In contrast, the Act is subject to the normal legislative process and is likely to be the subject of future hotly-contested amendment efforts. In the meantime, any business that collects or uses the personal information of California consumers should promptly assess a revamping of its compliance system and relationships with entities with which it shares

consumer information – including determining whether to apply the stringent California standards nationwide.

The attorneys of Stroock's Financial Services Litigation, Regulation and Enforcement Group are well positioned to answer any questions that you may have about the scope and impact of the Act, as well as related issues.

For More Information

Julia B. Strickland
310.556.5806
jstrickland@stroock.com

Quyen Truong
202.739.2888
qtruong@stroock.com

Stephen J. Newman
310.556.5982
snewman@stroock.com

Brian C. Frontino
305.789.9343
bfrontino@stroock.com

Arjun P. Rao
310.556.5822
arao@stroock.com

Ian DiBernardo
212.806.5867
idibernardo@stroock.com

New York
180 Maiden Lane
New York, NY 10038-4982
Tel: 212.806.5400
Fax: 212.806.6006

Los Angeles
2029 Century Park East
Los Angeles, CA 90067-3086
Tel: 310.556.5800
Fax: 310.556.5959

Miami
Southeast Financial Center
200 South Biscayne Boulevard, Suite 3100
Miami, FL 33131-5323
Tel: 305.358.9900
Fax: 305.789.9302

Washington, DC
1875 K Street NW, Suite 800
Washington, DC 20006-1253
Tel: 202.739.2800
Fax: 202.739.2895

www.stroock.com

Stroock & Stroock & Lavan LLP provides strategic transactional, regulatory and litigation advice to advance the business objectives of leading financial institutions, multinational corporations and entrepreneurial businesses in the U.S. and globally. With a rich history dating back 140 years, the firm has offices in New York, Los Angeles, Miami and Washington, D.C.

For further information about *Stroock Special Bulletins*, or other Stroock publications, please contact publications@stroock.com.